



## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<b>(51) International Patent Classification <sup>7</sup> :</b> <b>G07D 7/12, B41M 3/14</b>	<b>A1</b>	<b>(11) International Publication Number:</b> <b>WO 00/62258</b> <b>(43) International Publication Date:</b> 19 October 2000 (19.10.00)
<b>(21) International Application Number:</b> PCT/US00/08867 <b>(22) International Filing Date:</b> 3 April 2000 (03.04.00)  <b>(30) Priority Data:</b> 09/291,537           14 April 1999 (14.04.99)       US 09/524,441           14 March 2000 (14.03.00)       US  <b>(71) Applicant:</b> THE STANDARD REGISTER COMPANY [US/US]; 600 Albany Street, Dayton, OH 45408 (US).  <b>(72) Inventors:</b> THAXTON, Daniel, D.; 14582 Little Richmond Road, New Lebanon, OH 45345 (US). MOWRY, William, H., Jr.; 403 Volusia Avenue, Dayton, OH 45409 (US). HILL, Russell, E.; 503 Van Eaton Road, Xenia, OH 45385 (US).  <b>(74) Agents:</b> BEYER, James, E. et al.; Killworth, Gottman, Hagan & Schaeff, L.L.P., One Dayton Centre, Suite 500, One South Main Street, Dayton, OH 45402-2023 (US).		<b>(81) Designated States:</b> AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).  <b>Published</b> <i>With international search report.</i>
<b>(54) Title:</b> SECURITY DOCUMENT AUTHENTICATION		
<b>(57) Abstract</b>		
<p>A security document and a device for authenticating the security document are provided. The device for authenticating the security document comprises an optical imaging device and a specially programmed controller. The security document comprises a unique combination of covert triggers, overt triggers, and overt secure document indicators arranged to enhance the security of the document at issue and enable high speed machine authentication of the document at issue. In accordance with one embodiment of the present invention, a device for authenticating a security document is provided. The security document includes a security image printed on a face thereof. The security image is defined by a collection of security image elements and defines at least one document authentication scheme. The document authentication scheme is arranged to provide a primary indication of document authenticity. The authentication device comprises an optical imaging device and a specially programmed controller.</p>		

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakhstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

## SECURITY DOCUMENT AUTHENTICATION

The present invention relates to security documents and, more particularly, to security documents including enhanced means for authenticating the security  
5 document.

Conventional security documents, e.g., the void pantograph security documents and the varying tone security documents of U.S. Patents 4,579,370, 5,149,140, 5,197,765, 5,340,159, incorporate a security image designed to provide an indication of document authenticity on an attempted duplicate of the document. Often, the nature  
10 of the document authentication scheme is described in fine print along the top or bottom of the document -- "CASH ONLY WHEN THE COLORED AREA OF THIS DOCUMENT CHANGES GRADUALLY AND EVENLY FROM DARKER TO LIGHTER WITH THE DARKER AREA AT THE TOP" or "THE FACE OF THIS CHECK HAS A SECURITY VOID BACKGROUND PATTERN -- DO NOT CASH IF VOID IS VISIBLE." Unfortunately, these printed messages are readily apparent and can be very  
15 useful to a potential counterfeiter. Further, these printed message do little to enhance the security of the document on which they are printed and are typically not well-suited for high speed machine authentication.

Accordingly, there is a need for a security document that eliminates the need for readily apparent printed descriptions of the authentication schemes embodied in a  
20 document. Further, there is continuing need for security documents incorporating enhanced security features that are well-suited for high speed machine authentication. Finally, there is a need for a device for authenticating such a document.

This need is met by the present invention wherein a security document and a  
25 device for authenticating the security document are provided. The device for authenticating the security document comprises an optical imaging device and a specially programmed controller. The security document comprises a unique combination of covert triggers, overt triggers, and overt secure document indicators arranged to enhance the security of the document at issue and enable high speed  
30 machine authentication of the document at issue.

In accordance with one embodiment of the present invention, a device for authenticating a security document is provided. The security document includes a

security image printed on a face thereof. The security image is defined by a collection of security image elements and defines at least one document authentication scheme. The document authentication scheme is arranged to provide a primary indication of document authenticity. The authentication device comprises an optical imaging device  
5 and a specially programmed controller.

The optical imaging device is arranged to generate a security image signal representative of at least a portion of the security image. The controller is programmed to (i) define an authentication constellation within the security image, wherein the authentication constellation defines a set of constellation pixels, and wherein the  
10 constellation pixels are arranged at predetermined coordinates within the security image; (ii) identify respective occupation characteristics of each of the constellation pixels based on the security image signal, wherein each of the respective occupation characteristics represents a degree of printed matter within a selected constellation pixel; and (iii) determine whether the respective identified occupation characteristics  
15 correspond to an authentic document by comparing the respective identified occupation characteristics to a set of authentic occupation characteristics.

The security document may include a covert trigger defined by a set of covert trigger elements on the face of the security document and the controller may be programmed to identify the respective occupation characteristics based on printed  
20 matter defined by at least a portion of the covert trigger.

The controller may be programmed to identify the respective occupation characteristics based on printed matter defined by at least a portion of the security image. The security document preferably includes a covert trigger defined on the face of the security document and the controller is preferably programmed to identify the  
25 respective occupation characteristics based on printed matter defined by the covert trigger and the security image.

In accordance with another embodiment of the present invention, a device for authenticating a document is provided. The document includes an image printed on a face thereof. The image is defined by a collection of image elements. The  
30 authentication device comprises an optical imaging device and a specially programmed controller. The optical imaging device is arranged to generate an image signal representative of at least a portion of the image.

The controller is programmed to (i) define an authentication constellation within the image, wherein the authentication constellation defines a set of constellation pixels, and wherein the constellation pixels are arranged at predetermined coordinates within the image; (ii) identify respective occupation characteristics of each of the constellation  
5 pixels based on the image signal, wherein each of the respective occupation characteristics represents a degree of printed matter within a selected constellation pixel; and (iii) determine whether the respective identified occupation characteristics correspond to an authentic document by comparing the respective identified occupation characteristics to a set of authentic occupation characteristics.

10 In accordance with yet another embodiment of the present invention, a security document is provided comprising a security image and a covert trigger printed on a face of the document. The security image is defined by a collection of security image elements. The security image defines at least one document authentication scheme. The document authentication scheme is arranged to provide an indication of document  
15 authenticity. The covert trigger is defined by a collection of trigger elements. The trigger elements are arranged to resemble the security image elements so the covert trigger is not readily apparent on the face of the document. Preferably, the covert trigger elements and the security image elements are constructed of shapes having substantially identical geometry. The document authentication scheme may comprise  
20 a scheme selected from a void pantograph, an optically decodable security image, a varying tone security image, and combinations thereof.

The covert trigger may be arranged to provide an indication of document authenticity in addition to the indication of document authenticity provided by the document authentication scheme. If the security document includes at least one  
25 variable data field, the covert trigger may define an authentication parameter for the at least one data field. The variable data field may comprise a date field and the authentication parameter defined by the covert trigger may comprise an encoded date. Alternatively, the variable data field may comprise an amount field and the authentication parameter defined by the covert trigger may comprise a maximum  
30 amount limit.

The covert trigger may also be arranged to match a predetermined authentication mask or to identify the document authentication scheme.

The security document may further comprise an overt trigger arranged to be visually distinct from the security image elements. The overt trigger may also be arranged to provide an indication of document authenticity or to identify the document authentication scheme. Specifically, the overt trigger may include an encoded  
5 identification of the document authentication scheme. Alternatively, the overt trigger arrangement and the covert trigger arrangement may define substantially identical graphical images.

An overt secure document indicator may be arranged to be visually distinct from the security image elements and to provide a readily apparent indication that the  
10 document at issue includes enhances security features. The overt secure document indicator may comprise a graphical icon.

A security document according to the present invention may include a pseudo-covert trigger printed on the face of the document. The pseudo-covert trigger may be arranged as a decoy by printing it such that it is more apparent on the face of the  
15 document than the covert trigger and such that its elements are arranged to resemble the security image elements to a significantly lesser extent than the collection of trigger elements.

In accordance with yet another embodiment of the present invention, a method of authenticating a security document is provided. The security document at issue  
20 includes a security image printed on a face of the document. The security image includes a collection of security image elements and defines at least one document authentication scheme arranged to provide a primary indication of document authenticity. The method comprises the steps of: (i) defining an authentication constellation within the security image, wherein the authentication constellation defines  
25 a set of constellation pixels, and wherein the constellation pixels are arranged at predetermined coordinates within the security image; (ii) identifying respective occupation characteristics of each of the constellation pixels, wherein each of the respective occupation characteristics represents a degree of printed matter within a selected constellation pixel; and (iii) determining whether the respective identified  
30 occupation characteristics correspond to an authentic document by comparing the respective identified occupation characteristics to a set of authentic occupation characteristics.

A predetermined number of the authentic occupation characteristics may represent a degree of printed matter defined by a covert trigger defined on the face of the security document or by the security image itself. A predetermined number of the authentic occupation characteristics may represent an absence of printed matter within one of the selected constellation pixels. The step of identifying respective occupation characteristics of each of the constellation pixels may be executed by an automated machine.

In accordance with yet another embodiment of the present invention, a method of authenticating a document is provided. The document at issue includes an image printed on a face of the document. The image includes a collection of image elements. The method comprises the steps of: (i) defining an authentication constellation within the image, wherein the authentication constellation defines a set of constellation pixels, and wherein the constellation pixels are arranged at predetermined coordinates within the image; (ii) identifying respective occupation characteristics of each of the constellation pixels, wherein each of the respective occupation characteristics represents a degree of printed matter within a selected constellation pixel; and (iii) determining whether the respective identified occupation characteristics correspond to an authentic document by comparing the respective identified occupation characteristics to a set of authentic occupation characteristics.

In accordance with yet another embodiment of the present invention, a method of producing a security document is provided comprising the steps of: (i) defining a security image including a collection of security image elements, wherein the security image embodies a predetermined document authentication scheme arranged to provide an indication of document authenticity; (i) defining a covert trigger including a collection of trigger elements, wherein the trigger elements are arranged to resemble the security image elements; (ii) defining a trigger mask, wherein the trigger mask is arranged to define respective non-printed portions aligned with each of the trigger elements, and wherein each of the non-printed portions defines a non-printed buffer zone surrounding a corresponding trigger element; (iii) constructing a printed image from each of the security image, the covert trigger, and the trigger mask; and (iv) printing the constructed printed image on a substrate. The security image may include a background image layer, a message layer, a message layer mask, and a camouflage

image layer.

Accordingly, it is an object of the present invention to provide an enhanced security document and security document authentication scheme that eliminates the need for printing readily apparent descriptions of a document's security features on the document itself and satisfies the continuing need for security documents incorporating enhanced security features. Other objects of the present invention will be apparent in light of the description of the invention embodied herein.

The following detailed description of the preferred embodiments of the present invention can be best understood when read in conjunction with the following drawings, where like structure is indicated with like reference numerals and in which:

Fig 1 is a schematic illustration of a security document according to the present invention;

Fig. 2 is a schematic illustration of a security document according to an alternative embodiment of the present invention;

Figs. 3-6 are illustrations of a covert trigger and a method of document authentication according to the present invention;

Fig. 7 is an illustration of a method of producing a security document according to the present invention; and

Fig. 8 is a schematic illustration of a device for authenticating a security document according to the present invention.

Referring initially to Fig. 1, a security document 10 according to one embodiment of the present invention is illustrated. The security document 10 may be a negotiable instrument or another type of document including particular security features arranged to provide an indication of document authenticity. The illustrated security document includes a security image 20 printed on a front face 12 of the document 10. Although the security image 20 is merely illustrated schematically in Fig. 1, it will be understood by those practicing the present invention and familiar with security documents in general, including those described in U.S. Patents 4,579,370, 5,149,140, 5,197,765, 5,340,159, that the security image 20 is defined by a collection of security image elements 22. A set of security image elements 22 are illustrated schematically



-7-

in Fig. 3.

The security image 20 defines a predetermined document authentication scheme that provides an indication of document authenticity. For example, the security image may be a conventional void pantograph security image, an optically decodable security image, a varying tone security image, some other security image, or combinations thereof. For the purposes of describing and defining the present invention, it is noted that printed matter comprises any type of graphical representations reproduced on a substrate, regardless of the method by which the graphical representation is rendered on the substrate.

Referring now to Fig. 3, a covert trigger 30 is printed on the face 12 of the document 10. The covert trigger 30 is defined by a collection of trigger elements 32 and is referred to herein as a "covert" trigger because the trigger elements 32 are arranged to resemble the security image elements 22 such that the covert trigger 30 is not readily apparent on the face 12 of the document 10. Preferably, the covert trigger elements 32 and the security image elements 22 are constructed of shapes having substantially identical geometry, e.g., printed dots, clusters of printed dots, etc. It is contemplated by the present invention, however, that the covert trigger elements 32 and the security image elements 22 need not be identical. Rather, all that is required is that the covert trigger elements 32 be sized and positioned such that they are substantially hidden within the security image 20 so as not to be readily apparent upon casual inspection of the security document 10. In certain embodiments of the present invention, the covert trigger may be defined by partial printed elements, removed security image elements, or non-printed portions of the security image 20. In other embodiments of the present invention, a plurality of covert triggers 30 are provided across the face 12 of the document 10. The plural covert triggers 30 may be identical or distinct.

The covert trigger 30 may be arranged to provide an indication of document authenticity, to identify the document authentication scheme, or both. If the covert trigger 30 is arranged to provide an indication of document authenticity, that indication of authenticity will typically be in addition to the indication of document authenticity provided by the document authentication scheme.

In one embodiment of the present invention, the covert trigger 30 may be arranged such that it defines an authentication parameter for a data field on the security document 10. Specifically, the shape, appearance, or arrangement of the trigger 30 may be an encoded representation of a predetermined parameter against which the authenticity of the data field may be checked. For example, the variable data field may comprise a printed issue date and the authentication parameter defined by the covert trigger 30 may comprises an encoded expiration date against which the printed date may be checked. In this manner, a security document processor may guard against alteration of the security document issue date by reading the encoded expiration date. As a further example, the variable data field may comprise a printed amount and the authentication parameter defined by the covert trigger 30 may comprise an encoded maximum amount limit. In this manner, a security document processor may guard against alteration of the value of a negotiable document beyond the encoded maximum value.

In another embodiment of the present invention, the covert trigger 30 is arranged to identify the document authentication scheme. Specifically, the arrangement of the covert trigger 30 may be such that it provides an indication as to the nature of the one or more authentication schemes embodied in the security document 10. In this manner, the covert trigger 30 overcomes the disadvantages of merely describing the nature of the document authentication scheme in fine print along the top or bottom of the document -- "CASH ONLY WHEN THE COLORED AREA OF THIS DOCUMENT CHANGES GRADUALLY AND EVENLY FROM DARKER TO LIGHTER WITH THE DARKER AREA AT THE TOP" or "THE FACE OF THIS CHECK HAS A SECURITY VOID BACKGROUND PATTERN - DO NOT CASH IF VOID IS VISIBLE."

Referring again to Fig. 1, an overt trigger 40 is provided to further enhance the security document 10. The overt trigger 40 is arranged to be visually distinct from the security image elements such that it is readily viewable on the face 12 of the security document 10. The overt trigger 40 may be arranged to identify the document authentication scheme by defining an encoded identification of the nature of the authentication scheme embodied in the security document 10. For example, the numerals "6545382" printed on the face of the document 10 may correspond to a predetermined security document decoding algorithm or authentication algorithm, i.e.,

an algorithm that points to a specific machine-readable decoding or authentication scheme. It is contemplated by the present invention that the overt trigger 40 may be positioned in a portion of the document dedicated to the identification of security features embodied in the document 10. The portion of the document dedicated to the identification of security features, i.e., the security features rectangle, may be designated in an industry standard location.

The overt trigger 40 may also be arranged to provide an indication of document authenticity. For example, the overt trigger 40 and the covert trigger 30 may be arranged to define substantially identical graphical images. An indication as to document authenticity could be gleaned from a comparison of the respective graphical images defined by the overt trigger 40 and the covert trigger 30. For example, the covert trigger could be arranged to define the shape of the number "5" or a star shape and the overt trigger could be a printed number "5" or a star.

Referring now to Fig. 2, an overt secure document indicator 50 may also be printed on the face 12 of the security document 10 and is arranged to be visually distinct from the security image elements 22 so as to be readily apparent on the face of the document. Preferably, the overt secure document indicator 50 comprises a graphical icon that clearly identifies the document 10 as an enhanced security document. In the illustrated embodiment, for example, the overt secure document indicator 50 comprises a graphical representation of a pair of handcuffs. Other examples include a key, a lock, a chain link or a concertina wire pattern, etc.

Referring further to Figs. 2 and 3, another aspect of the present invention contemplates the addition of a printed pseudo-covert trigger 60 on the face 12 of the document 10. The pseudo-covert trigger is arranged to be more apparent on the face 12 of the document 10 than the covert trigger 30 by constructing it of pseudo-covert trigger elements 62 that resemble the security image elements 22 to a significantly lesser extent than the collection of trigger elements 32. In a preferred embodiment of the present invention, the pseudo-covert trigger 60 is utilized as a decoy for the true covert trigger 30. Specifically, a counterfeiter aware of the presence of a covert trigger somewhere on the face 12 of the security document 10 may tend to mistake the pseudo-covert trigger 60 as the covert trigger 30. As a result, the counterfeiter will copy the pseudo-covert trigger 60 instead of the covert trigger 30 and the resulting

-10-

invalid copy will be identifiable as an invalid document because the covert trigger 30 will not have been copied. As will be appreciated by those practicing the present invention, the pseudo-covert trigger 60 need not convey any particular meaning or be arranged in any specific manner because it is merely a phony trigger. For the purposes  
5 of describing and defining the present invention, it is noted that a true trigger is graphical image or collection of printed elements arranged to provide a direct indication of document authenticity or to indicate a means by which a document may be authenticated.

Referring to Figs. 3-6, various methods of authenticating a security document  
10 according to the present invention are illustrated. The security document at issue may or may not include a covert trigger, an overt trigger, a pseudo-covert trigger, or an overt secure document indicator. Rather, the security document at issue may merely include a security image 20 printed on a face of the document. The security image 20, which is illustrated only partially in Figs. 3-6, is defined by a collection of security image  
15 elements 22 and defines at least one document authentication scheme. The document authentication scheme, as is described above, is arranged to provide a primary indication of document authenticity. Initially, the method of authentication comprises the step of defining an authentication constellation 70 within the security image 20. The authentication constellation 70 defines a set of constellation pixels 72  
20 arranged at predetermined coordinates within the security image 20. It is noted that seven constellation pixels 72 are present in the embodiments of Figs. 3 and 5, ten constellation pixels 72 are present in the embodiment of Fig. 4, and nine constellation pixels 72 are present in the embodiment of Fig. 6.

In the embodiment illustrated in Fig. 3, the constellation pixels 72 are positioned  
25 to correspond to the positions of the trigger elements 32. However, as is implied above, the constellation pixels 72 need not be positioned to correspond to the positions of the trigger elements 32. Rather, as is illustrated in Figs. 4-6, the constellation pixels 72 may be arranged such that their positions correspond to the locations of security image elements 22 and trigger elements 32 (see Figs. 4 and 6), removed or missing security  
30 image elements 34 (see Figs. 4-6), other non-printed portions 36 of the security image 20 (see Figs. 4-6), or other combinations and selections of distinctive portions of printed or non-printed matter on the face of the security document at issue.

Once the authentication constellation 70 is identified, according to the authentication method of the present invention, the respective occupation characteristics of each of the constellation pixels 72 is identified. Each of the respective occupation characteristics represents a measure of the degree of printed matter within a selected constellation pixel 72. The document at issue may then be authenticated based upon a determination of whether the respective occupation characteristics correspond to the predetermined authentic occupation characteristics of a document. As will be appreciated by those practicing the authentication method of the present invention, it will be preferable to establish a degree of tolerance in comparing the respective occupation characteristics with the corresponding predetermined authentic occupation characteristics of a document. For example, it may be preferable to authenticate a document if the 90% of the identified occupation characteristics correspond to the predetermined authentic occupation characteristics.

As is noted above, the covert trigger 30 itself may be arranged to match a predetermined authentication mask defining the authentication constellation 70. For the purposes of defining and describing the present invention, it is noted that the noted "degree of printed matter" includes the case where no printed matter is included within a selected constellation pixel 72.

As is noted above, the step of identifying respective occupation characteristics of each of the constellation pixels may be executed by an automated machine. More specifically, referring to Fig. 8, in accordance with one embodiment of the present invention, a device 80 for authenticating a security document is provided. The authentication device 80 comprises a specially programmed controller 82 and an optical imaging device 84.

The authentication device 80 may be utilized in a variety of applications. For example, the authentication device may be utilized with various types of security document or check processing equipment, like reader/sorters and point of sale terminals, to enable authentication when security documents or checks are in various stages of processing. In preferred embodiments of the present invention, the authentication device 80 is utilized at a check's point of first presentment, e.g., a point of sale terminal or a teller terminal at a banking or check cashing institution. The authentication device 80 may be positioned near or mounted to the check processing

equipment. However, in a preferred embodiment of the present invention the authentication device 80 is incorporated directly into the internal structure of the equipment and is arranged to share hardware and software resources with the equipment.

5       The optical imaging device 84 is arranged to generate a security image signal representative of at least a portion of the security image. Regarding the specific arrangement of the imaging device 84, it is noted that any one of a number of commercially available imaging devices may be modified or adapted in accordance with the teachings of the present invention. Preferably, the device 84 includes a high  
10 resolution optics assembly capable of scanning a security document and generating the security image signal with the aid of a suitably programmed controller. Examples of imaging devices that may be arranged for operation according to the present invention include the IT9000E and the IT9000T imagers and the 4400HD/HD10 hand-held image readers available from Welch Allyn data collection Skaneateles Falls, NY  
15 and the RDM EC5000i, available from the RDM Corporation, Waterloo, Ontario.

      The controller 82 is programmed to define the authentication constellation 70 within the security image 20 and identify respective occupation characteristics of each of the constellation pixels 72 based on the security image signal. The controller 82 is further programmed to determine whether the respective identified occupation  
20 characteristics correspond to an authentic document by comparing the respective identified occupation characteristics to a set of authentic occupation characteristics. Where the security document includes a covert trigger 30 the controller 82 is programmed to identify the respective occupation characteristics based on printed matter defined by the covert trigger 30, the security image 20, or combinations thereof.

25       Referring now to Fig. 7, a method of producing a security document according to the present invention is illustrated schematically. Initially, a digital security image is defined, typically utilizing suitable graphic design software. The security image includes a collection of security image elements and embodies a predetermined document authentication scheme, referred to above, which is arranged to provide an  
30 indication of document authenticity. As is illustrated in Fig. 7, the security image includes: (i) a background image layer 102; (ii) a message layer 106; (iii) a message layer mask 104 defining non-printed areas within the background layer 102

-13-

corresponding to the positions of the printed matter within the message layer 106; and  
(iv) a camouflage image layer 108 further defining non-printed matter arranged to obscure the message layer 106.

A covert trigger layer 112 is also defined and includes a collection of trigger  
5 elements. As is noted above, the trigger elements may comprise printed elements, partial printed elements, or non-printed space. In any event, the trigger elements of the covert trigger layer 112 are preferably arranged to resemble the security image. A trigger mask layer 110 is defined and is arranged to define respective non-printed portions aligned with each of the trigger elements in the covert trigger layer 112. Each  
10 of the non-printed portions in the trigger mask layer 110 defines a non-printed buffer zone surrounding a corresponding trigger element in the covert trigger layer 112. The buffer zone is most conveniently provided by ensuring that the non-printed portions of the trigger mask layer 110 are aligned with, and uniformly larger than, the trigger elements in the covert trigger layer 112. The buffer zone of the trigger mask layer 110  
15 provides for a margin of error in positioning the elements of the covert trigger layer 112. The image to be printed on the substrate 100 is constructed from the background image layer 102, the message layer 106, the message layer mask 104, the camouflage image layer 108, the trigger mask layer 110, and the covert trigger layer 112.

Having described the invention in detail and by reference to preferred  
20 embodiments thereof, it will be apparent that modifications and variations are possible without departing from the scope of the invention defined in the appended claims.

-14-

## CLAIMS

1. A security document comprising:
  - a security image printed on a face of said document, wherein said security image is defined by a collection of security image elements, wherein said security image defines at least one document authentication scheme, and wherein said document authentication scheme is arranged to provide an indication of document authenticity; and
  - a covert trigger printed on said face of said document, wherein said covert trigger is defined by a collection of trigger elements, wherein said trigger elements are arranged to resemble said security image elements such that said covert trigger is not readily apparent on said face of said document.
2. A security document as claimed in claim 1 wherein said covert trigger elements and said security image elements are constructed of shapes having substantially identical geometry.
3. A security document as claimed in claim 1 wherein said document authentication scheme comprises a scheme selected from one or more of a void pantograph, an optically decodable security image, a varying tone security image, and combinations thereof.
4. A security document as claimed in claim 1 wherein said covert trigger is arranged to provide an indication of document authenticity in addition to the indication of document authenticity provided by said document authentication scheme.
5. A security document as claimed in claim 4 wherein said security document includes at least one variable data field and wherein said covert trigger defines an authentication parameter for said at least one data field.
6. A security document as claimed in claim 5 wherein said variable data field comprises a date field and wherein said authentication parameter defined by said covert trigger comprises an encoded date.



-15-

7. A security document as claimed in claim 5 wherein said variable data field comprises an amount field and wherein said authentication parameter defined by said covert trigger comprises a maximum amount limit.
- 5 8. A security document as claimed in claim 4 wherein said covert trigger is arranged to match a predetermined authentication mask.
9. A security document as claimed in claim 1 wherein said covert trigger is arranged to identify said document authentication scheme.
- 10 10. A security document as claimed in claim 1 further comprising an overt trigger arranged to be visually distinct from said security image elements, wherein said overt trigger is arranged to provide an indication of document authenticity.
- 15 11. A security document as claimed in claim 1 further comprising an overt trigger arranged to be visually distinct from said security image elements, wherein said overt trigger is arranged to identify said document authentication scheme.
12. A security document as claimed in claim 11 wherein said overt trigger includes an  
20 encoded identification of said document authentication scheme.
13. A security document as claimed in claim 1 further comprising an overt trigger arranged to be visually distinct from said security image elements, wherein said overt trigger arrangement and said covert trigger arrangement define substantially identical  
25 graphical images.
14. A security document as claimed in claim 1 further comprising an overt secure document indicator arranged to be visually distinct from said security image elements.
- 30 15. A security document as claimed in claim 14 wherein said overt secure document indicator comprises a graphical icon.

-16-

16. A security document as claimed in claim 1 further comprising a pseudo-covert trigger printed on said face of said document, wherein said pseudo-covert trigger is more apparent on said face of said document than said covert trigger, and wherein pseudo-covert trigger elements are arranged to resemble said security image elements  
5 to a significantly lesser extent than said collection of trigger elements.

17. A security document as claimed in claim 1 wherein said covert trigger elements are selected from one or more of a printed element, a partial printed element, and non-printed space.

10

18. A method of authenticating a security document including a security image printed on a face of said document, wherein said security image is defined by a collection of security image elements, wherein said security image defines at least one document authentication scheme, and wherein said document authentication scheme is arranged  
15 to provide a primary indication of document authenticity, said method comprising the steps of:

defining an authentication constellation within said security image, wherein said authentication constellation defines a set of constellation pixels, and wherein said constellation pixels are arranged at predetermined coordinates within said security  
20 image;

identifying respective occupation characteristics of each of said constellation pixels, wherein each of said respective occupation characteristics represents a degree of printed matter within a selected constellation pixel; and

determining whether said respective identified occupation characteristics  
25 correspond to an authentic document by comparing said respective identified occupation characteristics to a set of authentic occupation characteristics.

19. A method of authenticating a security document as claimed in claim 18 wherein a predetermined number of said authentic occupation characteristics represent a degree  
30 of printed matter defined by at least a portion of a covert trigger defined on said face of said security document.

20. A method of authenticating a security document as claimed in claim 18 wherein a predetermined number of said authentic occupation characteristics represent a degree of printed matter defined by at least a portion of said security image.

5 21. A method of authenticating a security document as claimed in claim 18 wherein a predetermined number of said authentic occupation characteristics represents a degree of printed matter defined by at least a portion of said security image and at least a portion of a covert trigger defined on said face of said security document.

10 22. A method of authenticating a security document as claimed in claim 18 wherein a predetermined number of said authentic occupation characteristics represent an absence of printed matter within one of said selected constellation pixels.

23. A method of authenticating a security document as claimed in claim 18 wherein  
15 said step of identifying respective occupation characteristics of each of said constellation pixels is executed by an automated machine.

24. A method of authenticating a document including an image printed on a face of said document, wherein said image is defined by a collection of image elements, said  
20 method comprising the steps of:

defining an authentication constellation within said image, wherein said authentication constellation defines a set of constellation pixels, and wherein said constellation pixels are arranged at predetermined coordinates within said image;

25 identifying respective occupation characteristics of each of said constellation pixels, wherein each of said respective occupation characteristics represents a degree of printed matter within a selected constellation pixel; and

determining whether said respective identified occupation characteristics correspond to an authentic document by comparing said respective identified occupation characteristics to a set of authentic occupation characteristics.

30

25. A method of authenticating a document as claimed in claim 24 wherein a predetermined number of said authentic occupation characteristics represents a

-18-

degree of printed matter defined by at least a portion of a covert trigger defined on said face of said document.

26. A method of authenticating a security document as claimed in claim 24 wherein a  
5 predetermined number of said authentic occupation characteristics represent a degree of printed matter defined by at least a portion of said image.

27. A method of authenticating a security document as claimed in claim 18 wherein a  
predetermined number of said authentic occupation characteristics represents a  
10 degree of printed matter defined by at least a portion of said image and at least a portion of a covert trigger defined on said face of said security document.

28. A method of authenticating a security document as claimed in claim 24 wherein a  
predetermined number of said authentic occupation characteristics represent an  
15 absence of printed matter within one of said selected constellation pixels.

29. A method of producing a security document comprising the steps of:  
defining a security image including a collection of security image elements,  
wherein said security image embodies a predetermined document authentication  
20 scheme arranged to provide an indication of document authenticity;  
defining a covert trigger including a collection of trigger elements, wherein said  
trigger elements are arranged to resemble said security image elements;  
defining a trigger mask, wherein said trigger mask is arranged to define  
respective non-printed portions aligned with each of said trigger elements, and wherein  
25 each of said non-printed portions defines a non-printed buffer zone surrounding a  
corresponding trigger element;  
constructing a printed image from each of said security image, said covert  
trigger, and said trigger mask; and  
printing said constructed printed image on a substrate.

30

30. A method of producing a security document as claimed in claim 29 wherein said security image includes a background image layer, a message layer, a message layer mask, and a camouflage image layer.

- 5 31. A device for authenticating a security document, said security document including a security image printed on a face thereof, wherein said security image is defined by a collection of security image elements, wherein said security image defines at least one document authentication scheme, and wherein said document authentication scheme is arranged to provide a primary indication of document authenticity, said
- 10 authentication device comprising:
- an optical imaging device arranged to generate a security image signal representative of at least a portion of said security image; and
  - a controller programmed to
    - 15 define an authentication constellation within said security image, wherein said authentication constellation defines a set of constellation pixels, and wherein said constellation pixels are arranged at predetermined coordinates within said security image;
    - identify respective occupation characteristics of each of said constellation pixels based on said security image signal, wherein each of
    - 20 said respective occupation characteristics represents a degree of printed matter within a selected constellation pixel; and
    - determine whether said respective identified occupation characteristics correspond to an authentic document by comparing said respective identified occupation characteristics to a set of authentic
    - 25 occupation characteristics.

32. A device for authenticating a security document as claimed in claim 31 wherein said security document includes a covert trigger defined by a set of covert trigger elements on said face of said security document and wherein said controller is
- 30 programmed to identify said respective occupation characteristics based on printed matter defined by at least a portion of said covert trigger.

-20-

33. A device for authenticating a security document as claimed in claim 31 wherein said controller is programmed to identify said respective occupation characteristics based on printed matter defined by at least a portion of said security image.

5 34. A device for authenticating a security document as claimed in claim 31 wherein said security document includes a covert trigger defined by a set of covert trigger elements on said face of said security document and wherein said controller is programmed to identify said respective occupation characteristics based on printed matter defined by said covert trigger and said security image.

10

35. A device for authenticating a security document as claimed in claim 31 wherein selected ones of said authentic occupation characteristics represent an absence of printed matter within one of said selected constellation pixels.

15 36. A device for authenticating a security document as claimed in claim 32 wherein said covert trigger elements and said security image elements are constructed of shapes having substantially identical geometry.

37. A device for authenticating a security document as claimed in claim 31 wherein  
20 said document authentication scheme comprises a scheme selected from one or more of a void pantograph, an optically decodable security image, a varying tone security image, and combinations thereof.

38. A device for authenticating a security document as claimed in claim 31 wherein  
25 said covert trigger is arranged to provide an indication of document authenticity in addition to the indication of document authenticity provided by said document authentication scheme.

39. A device for authenticating a security document as claimed in claim 38 wherein  
30 said security document includes at least one variable data field and wherein said covert trigger defines an authentication parameter for said variable data field.

40. A device for authenticating a security document as claimed in claim 39 wherein said variable data field comprises a date field and wherein said authentication parameter defined by said covert trigger comprises an encoded date.

5 41. A device for authenticating a security document as claimed in claim 39 wherein said variable data field comprises an amount field and wherein said authentication parameter defined by said covert trigger comprises a maximum amount limit.

42. A device for authenticating a security document as claimed in claim 31 wherein  
10 said covert trigger is arranged to match a predetermined authentication mask.

43. A device for authenticating a security document as claimed in claim 31 wherein said covert trigger is arranged to identify said document authentication scheme.

15 44. A device for authenticating a security document as claimed in claim 32 wherein said covert trigger elements are selected from one or more of a printed element, a partial printed element, and non-printed space.

45. A device for authenticating a security document as claimed in claim 31 wherein  
20 said optical imaging device comprises a high resolution optics assembly capable of scanning said security document.

46. A device for authenticating a security document as claimed in claim 31 wherein said optical imaging device is selected from a group comprising a linear imaging device  
25 and a hand-held imaging device.

47. A device for authenticating a document, said document including an image printed on a face thereof, wherein said image is defined by a collection of image elements, said authentication device comprising:  
30 an optical imaging device arranged to generate an image signal representative of at least a portion of said image; and

-22-

a controller programmed to

define an authentication constellation within said image, wherein said authentication constellation defines a set of constellation pixels, and wherein said constellation pixels are arranged at predetermined coordinates within said image;

identify respective occupation characteristics of each of said constellation pixels based on said image signal, wherein each of said respective occupation characteristics represents a degree of printed matter within a selected constellation pixel; and

determine whether said respective identified occupation characteristics correspond to an authentic document by comparing said respective identified occupation characteristics to a set of authentic occupation characteristics.

48. A security document processor comprising document processing hardware and a device for authenticating a security document, said security document including a security image printed on a face thereof, wherein said security image is defined by a collection of security image elements, wherein said security image defines at least one document authentication scheme, and wherein said document authentication scheme is arranged to provide a primary indication of document authenticity, said authentication device comprising:

an optical imaging device arranged to generate a security image signal representative of at least a portion of said security image; and

a controller programmed to

define an authentication constellation within said security image, wherein said authentication constellation defines a set of constellation pixels, and wherein said constellation pixels are arranged at predetermined coordinates within said security image;

identify respective occupation characteristics of each of said constellation pixels based on said security image signal, wherein each of said respective occupation characteristics represents a degree of printed matter within a selected constellation pixel; and



-23-

5                   determine whether said respective identified occupation  
                    characteristics correspond to an authentic document by comparing said  
                    respective identified occupation characteristics to a set of authentic  
                    occupation characteristics.

49. A security document processor as claimed in claim 48 wherein said device for  
                    authenticating said security document is mounted to said document processing  
10 hardware.

50. A security document processor as claimed in claim 48 wherein said device for  
                    authenticating said security document and said document processing hardware share  
                    common hardware resources.

15

51. A security document processor as claimed in claim 48 wherein said device for  
                    authenticating said security document and said document processing hardware share  
                    common software resources.

20

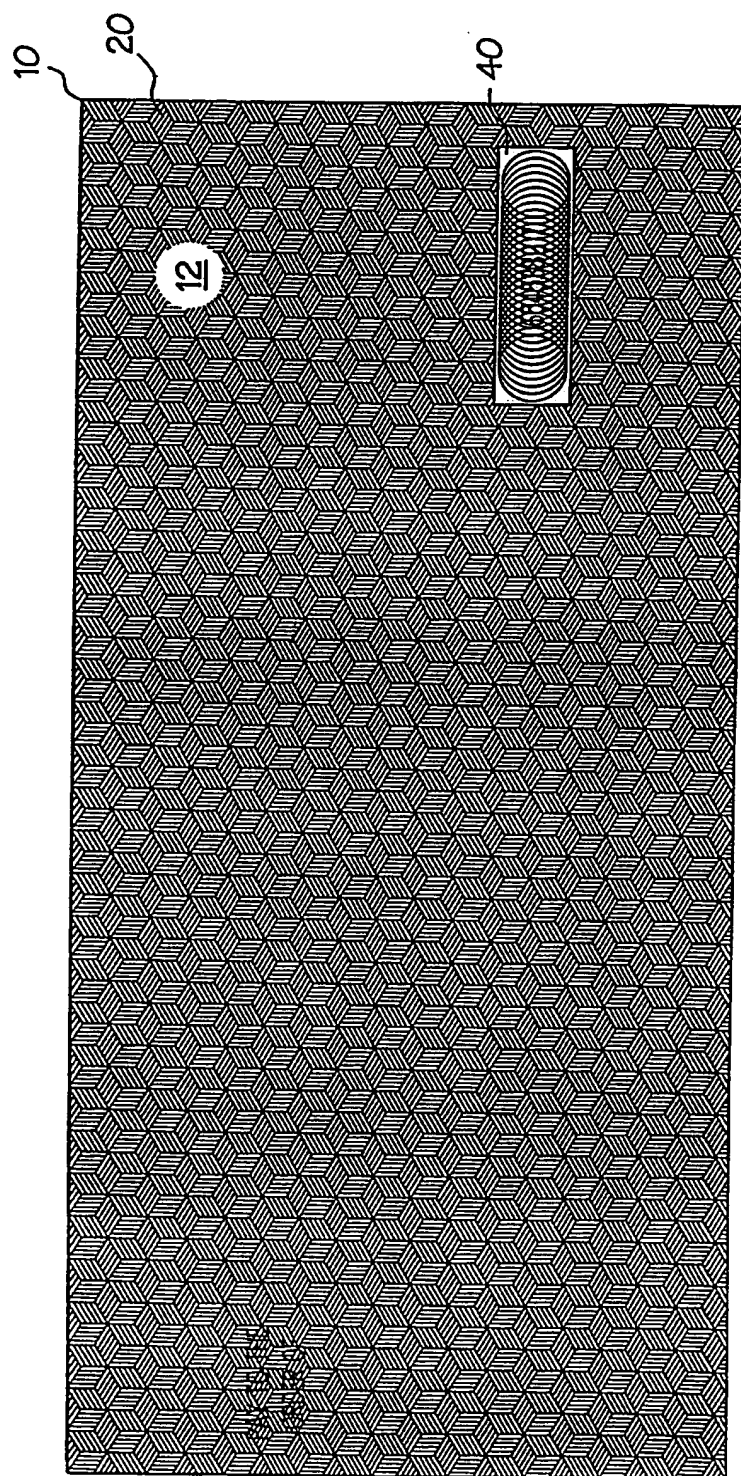


FIG. 1

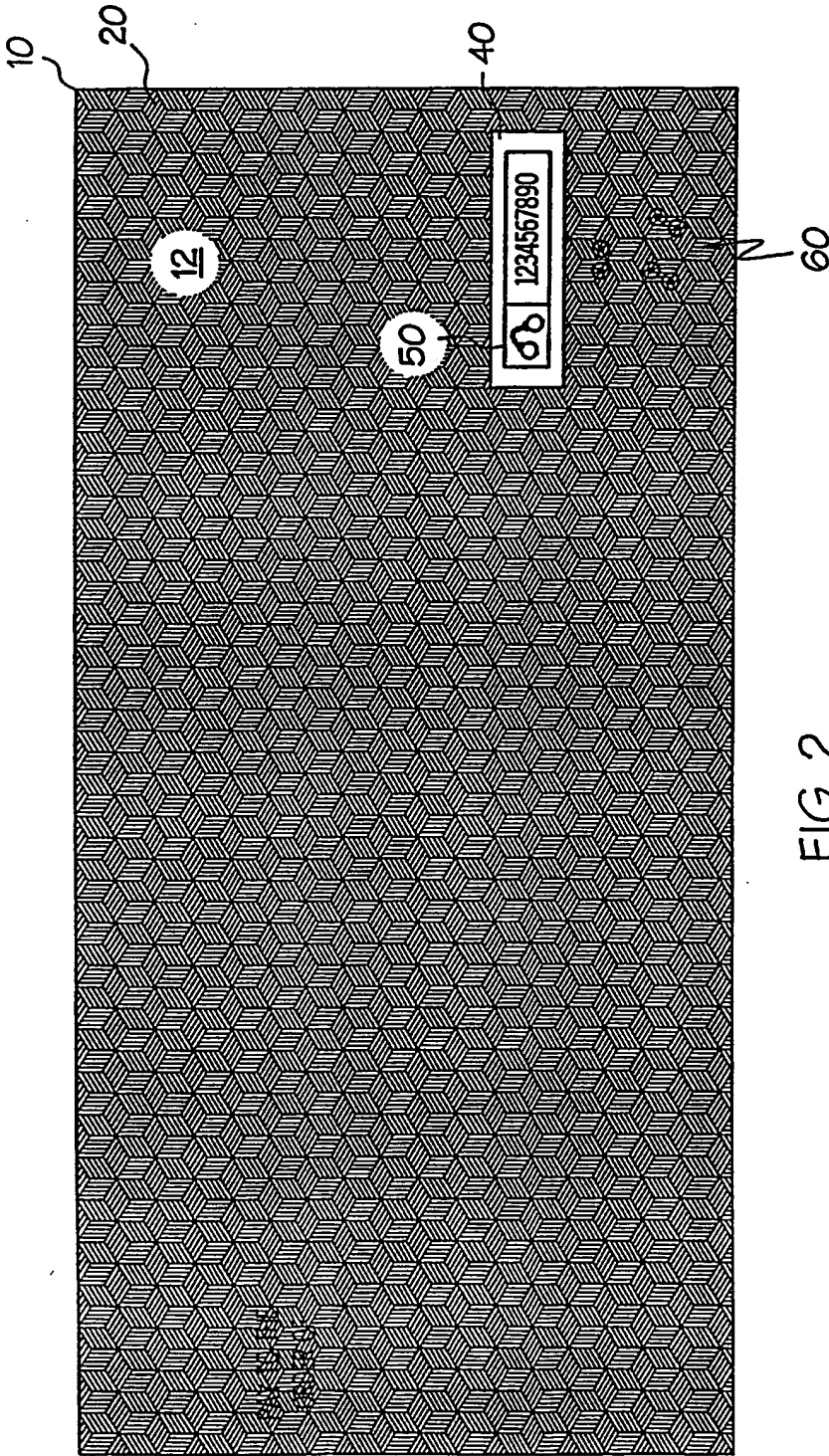


FIG. 2

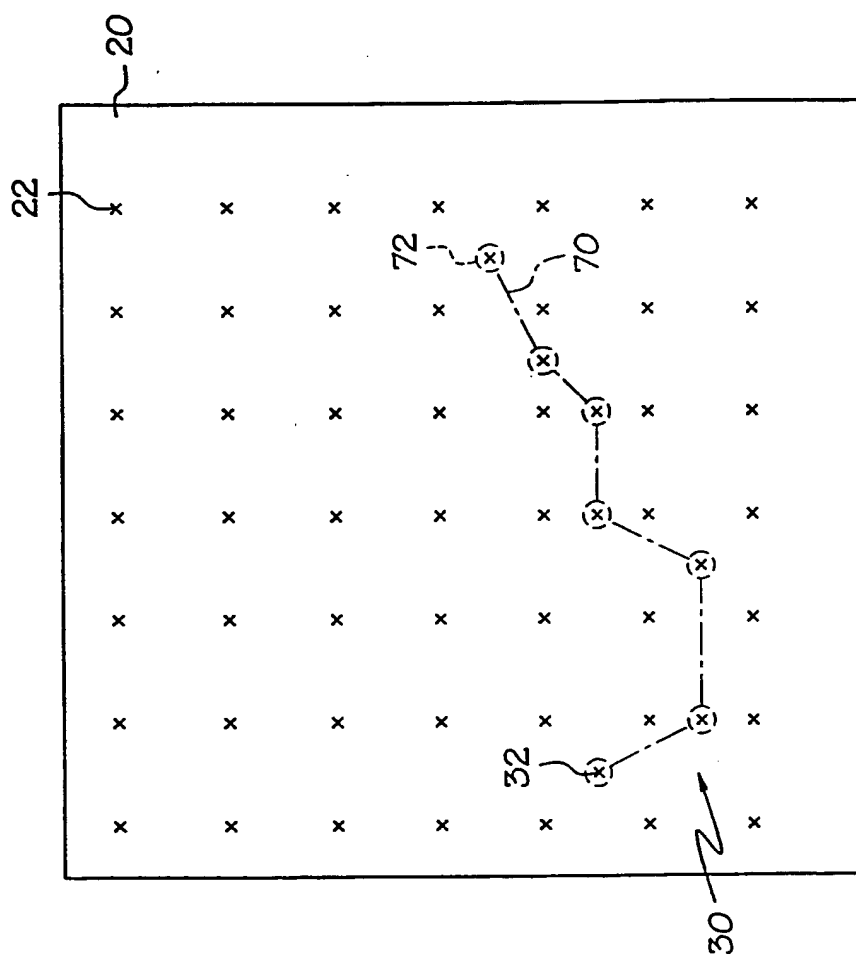


FIG. 3

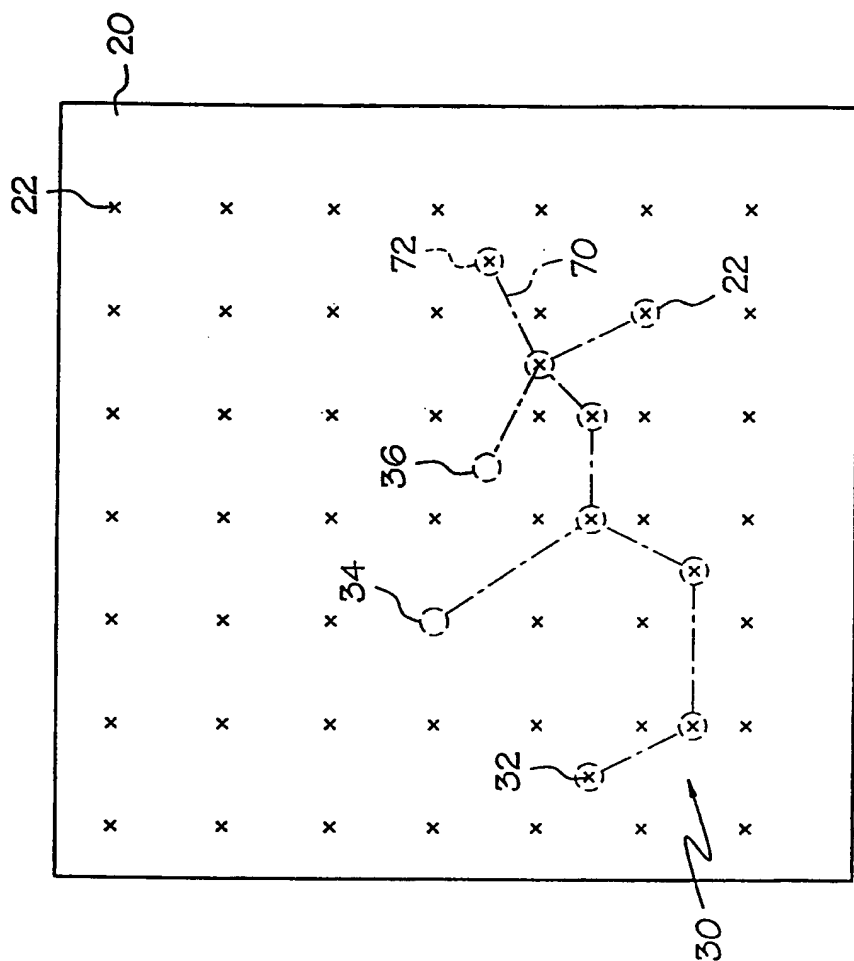


FIG. 4

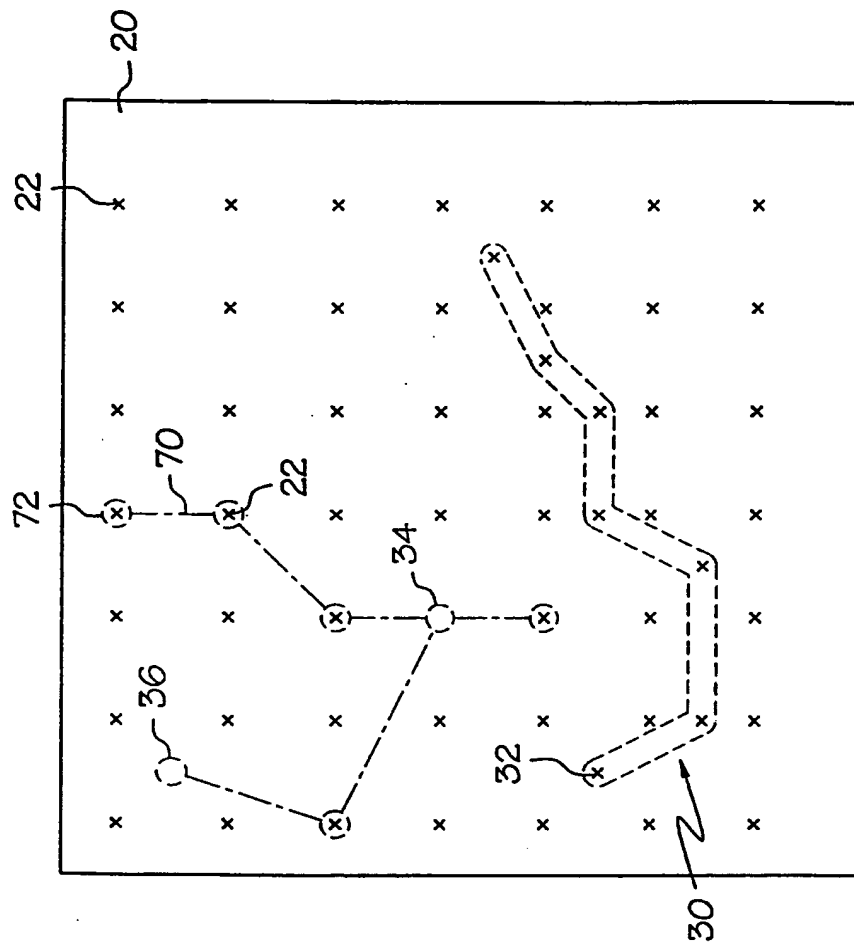


FIG. 5

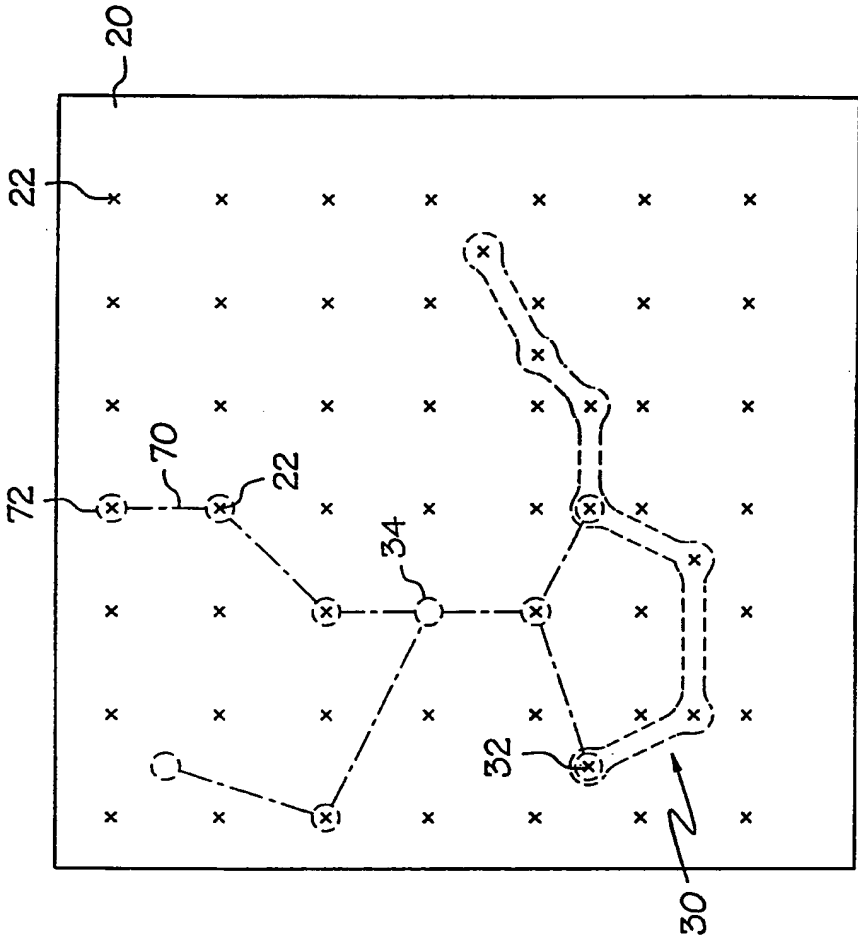


FIG. 6

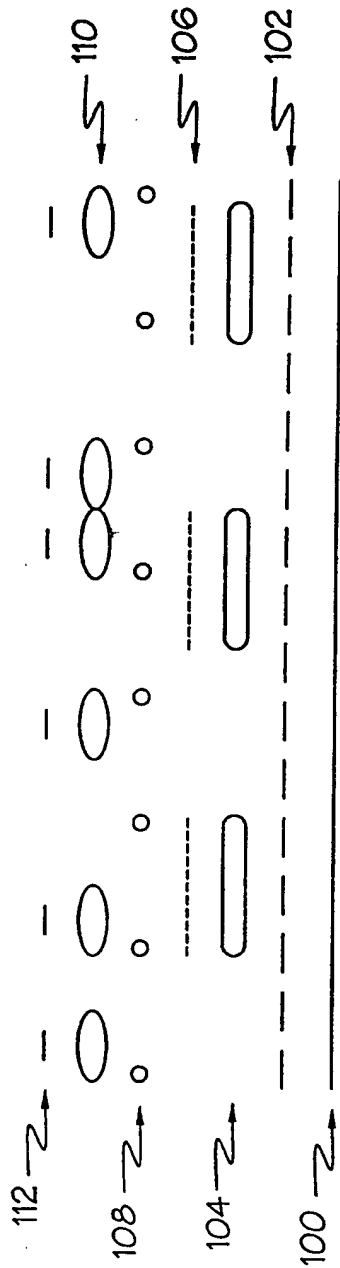
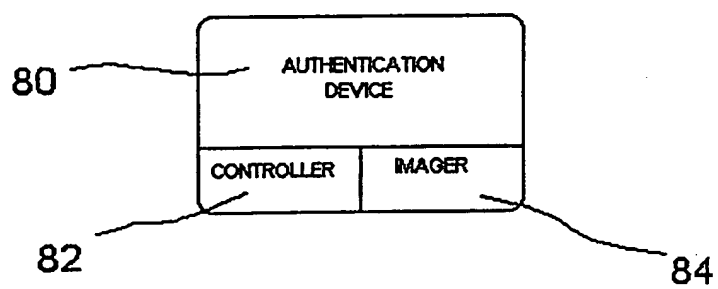


FIG. 7



Fig. 8



# INTERNATIONAL SEARCH REPORT

Intern. Application No  
PCT/US 00/08867

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 G07D/12 B41M3/14

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 G07D B41M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 22292 A (STANDARD REGISTER CO) 28 May 1998 (1998-05-28) page 11, line 10 -page 19, line 19 figures 4,5,10,11	1-4,17, 18,24,29
A	US 5 785 353 A (DIAMOND ROBERT I) 28 July 1998 (1998-07-28) the whole document	1-4,17, 29
A	US 5 621 810 A (KAWASE MICHIO ET AL) 15 April 1997 (1997-04-15) column 1, line 63 -column 2, line 50 figures 1,2,13-15,29	18,24, 31,47,48
A	US 5 647 010 A (OKUBO HIROMI ET AL) 8 July 1997 (1997-07-08) claims figures 1,2	31,47,48



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "8" document member of the same patent family

Date of the actual completion of the international search

7 July 2000

Date of mailing of the international search report

18/07/2000

Name and mailing address of the ISA  
European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Bocage, S

# INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/US 00/08867

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9822292 A	28-05-1998	US 5954368 A AU 5790298 A	21-09-1999 10-06-1998
US 5785353 A	28-07-1998	US 5575508 A US 5538290 A US 5984364 A US 5641183 A	19-11-1996 23-07-1996 16-11-1999 24-06-1997
US 5621810 A	15-04-1997	JP 2210481 A JP 2994655 B JP 2210591 A JP 2994656 B JP 2284189 A JP 2749866 B JP 2288468 A JP 2951964 B US 5426710 A US 5216724 A CA 2009699 A,C DE 69023782 D DE 69023782 T DE 69033327 D DE 69033327 T EP 0382549 A EP 0665477 A	21-08-1990 27-12-1999 21-08-1990 27-12-1999 21-11-1990 13-05-1998 28-11-1990 20-09-1999 20-06-1995 01-06-1993 10-08-1990 11-01-1996 13-06-1996 18-11-1999 13-04-2000 16-08-1990 02-08-1995
US 5647010 A	08-07-1997	JP 7087309 A JP 7273984 A DE 4432741 A	31-03-1995 20-10-1995 16-03-1995